

REMARKS

The present application was filed on April 5, 2001 with claims 1-20.

In the outstanding Office Action, the Examiner appears to maintain the provisional rejection of claims 1, 3-8, 10, 12-17, 19 and 20 under the judicially created doctrine of obviousness-type double patenting based on the copending U.S. patent application identified as Serial No. 09/638,320.

In response thereto, Applicant respectfully points out that a Terminal Disclaimer to Obviate a Provisional Double Patenting Rejection Over a Pending Reference Application was filed in Applicant's previous response on June 3, 2005. Such terminal disclaimer should serve to remove any obviousness-type double patenting rejection based on the U.S. patent application identified as Serial No. 09/638,320. Despite this fact, the Office Action is silent to the terminal disclaimer and appears to maintain the rejection. Applicant requests withdrawal of the obviousness-type double patenting rejection for at least the above reasons.

Furthermore, in the outstanding Office Action, the Examiner appears to reject claims 1, 3-8, 10, 12-17, 19 and 20 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,226,383 to Jablon (hereinafter "Jablon") in view of B. Schneier, "Applied Cryptography" (hereinafter "Schneier").

Applicants respectfully point out that it is well-established law that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 U.S.P.Q.2d 1051, 1053 (Fed. Cir. 1987) (Underlining added for emphasis). Thus, §102(e) rejection can not be based on Jablon in view of Schneier.

Further, despite the citation of Jablon in the §102(e) rejection, the actual rejection refers to "Schneier." However, it appears that this is a typographical error since the actual citations seem to correspond to Jablon.

Thus, to the degree that the §102(e) rejection is intended to be based merely on Jablon, Applicants traverse the rejection for at least the following reasons.

Regarding the §102(e) rejection of claims 1, 3-8, 10, 12-17, 19 and 20 based on Jablon, Applicant asserts that the rejection does not meet this basic legal requirement set out by the Federal Circuit in the above-cited *Verdegaal Bros.* decision, as will be explained below.

The present invention, for example, as recited in independent claim 1, comprises a method for communication via a data network, between two parties that share a password, using a Diffie-

Hellman type key exchange on a particular group to generate a shared secret g^{xy} , where g is the group generator known to both parties and x is an index known to one party and y is an index known to the other party, the group having a group operation and an inverse group operation. The method comprises the steps of one party generating a parameter m by performing the group operation on g^x and a function of at least the password, wherein any portion of a result associated with the function that is outside the group is randomized, and transmitting m to the other party, whereby the other party may perform the inverse group operation on m and the function of at least the password, and remove the randomization of any portion of the result associated with the function that is outside the group, to extract g^x and calculate the shared secret g^{xy} . Independent claims 10 and 19 recite similar limitations in accordance with apparatus and article of manufacture aspects of the invention. Independent claims 8, 17 and 20 respectively recite similar limitations as claims 1, 10 and 19 from the perspective of the "other party."

Jablon does not teach or suggest each and every element of the claimed invention. For example, Jablon does not teach or suggest "any portion of a result associated with the function that is outside the group is randomized . . . and remov[ing] the randomization of any portion of the result associated with the function that is outside the group," as recited in the claimed invention.

The Examiner appears to suggest (at page 5 of the Office Action) that Jablon at column 8, line 7, through column 9, line 12, discloses randomizing the part of a result lying outside the group, and subsequently removing that randomization. However, Jablon does not teach or suggest anything like that. In fact, Jablon appears to assume that the generator g used is "primitive" (see column 10, lines 50-51), and thus everything is inside the group, and nothing is outside the group. Therefore, it is not possible for Jablon to disclose randomizing something outside the group. With regard to the randomness that Jablon mentions on column 10, line 55, this appears to refer to a specific function of the password S^2 . Thus, it is quite clear that Jablon fails to teach or suggest "any portion of a result associated with the function that is outside the group is randomized . . . and remov[ing] the randomization of any portion of the result associated with the function that is outside the group," as recited in the claimed invention.


For at least the above reasons, Applicant asserts that claims 1, 3-8, 10, 12-17, 19 and 20 are patentable over Jablon.

Regarding claims 2, 9, 11 and 18, while the Office Action Summary page lists the claims as being objected to (and seemingly allowable), the body of the Office Action appears to make no

reference to them. Applicant thus requests clarification on the status of these claims.

In view of the above, Applicant believes that claims 1-20 are in condition for allowance, and respectfully requests withdrawal of the provisional double patenting and §102(e) rejections.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "William E. Lewis", written over the printed name.

Date: August 31, 2005

William E. Lewis
Attorney for Applicant(s)
Reg. No. 39,274
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-2946